Amendments to the Claims:

This listing of the claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for accessing encrypted data by a client, the method comprising ~~the steps of~~:

implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the sever secret, wherein the protocol is implemented so that the client cannot feasibly determine the sever secret and the server cannot feasibly determine the client secret or the third secret;

~~receiving by a server from a client client information derived from a first secret wherein the client information is derived such that the server can not feasibly determine the first secret;~~

~~providing to the client by the server intermediate data, the intermediate data derived responsive to at least the received client information and to a server secret, wherein the intermediate data is derived such that the client can not feasibly determine the server secret;~~

authenticating the client by a device, the device storing encrypted secrets and configured not to provide the encrypted secrets without authentication; and

after ~~the~~ authenticating ~~step~~, providing to the client by the device the encrypted secrets, wherein the encrypted secrets are capable of being decrypted using a decryption key derived from the third secret ~~that is derived from the intermediate data~~ and wherein the multi-party secure computation protocol implemented between the client and the server is the only multi-party computation protocol that is implemented in generating the third secret and the decryption key derived from the third secret.

2. (Currently Amended) The method of claim ~~1~~ 43 wherein the third secret is derived from the intermediate data by use of one of a key derivation function and a hash function.

3. (Currently Amended) The method of claim ~~1~~ 43 wherein the third secret is the intermediate data.

4. (Original) The method of claim 1 wherein the client ~~first~~ secret comprises at least one of a PIN, a password, and biometric information.

5. (Currently Amended) The method of claim ~~1~~ 43 wherein the intermediate data is derived from at least the client ~~first~~ secret and the server secret by use of a blind function evaluation protocol.

6. (Original) The method of claim 5 wherein the security of the blind function evaluation protocol is based on the problem of extracting roots modulo a composite.

7. (Original) The method of claim 5 wherein the security of the blind function evaluation protocol uses discrete logarithms.

8. (Currently Amended) The method of claim 1 wherein ~~the~~ authenticating ~~step~~ comprises authenticating the client based on a time-dependent code.

9. (Currently Amended) The method of claim 1 wherein ~~the~~ authenticating ~~step~~ comprises authenticating the client based on at least one of a PIN, a password, and biometric information.

10. (Currently Amended) The method of claim 1 wherein ~~the~~ authenticating ~~step~~ comprises authenticating the client based on a secret other than the ~~first~~ client secret.

11. (Currently Amended) The method of claim 1 wherein ~~the~~ authenticating ~~step~~ comprises using an authenticaion secret derived from the third secret ~~intermediate data~~.

12. (Original) The method of claim 1 wherein the device comprises at least one of a file server, a directory server, a key server, a PDA, a mobile telephone, a smart card, and a desktop computer.

13. (Original) The method of claim 12 wherein the device comprises at least one secure data store, the device requiring authentication before allowing the client access to the data store.

14. (Original) The method of claim 1 wherein the encrypted secrets comprise a private key of a public/private key pair used for asymmetric cryptography.

15. (Original) The method of claim 14 wherein the encrypted secrets comprise a signature key used for creating a digital signature.

16. (Currently Amended) The method of claim 15 wherein ~~the~~ authenticating ~~step~~ comprises authenticating the client based on a secret other than the first secret, so that the user provides different information to access the device and access the signature key.

17. (Original) The method of claim 1 wherein the encrypted secrets comprise a secret key used for symmetric cryptography.

18. (Original) The method of claim 1 wherein the encrypted secrets comprise at least one unit of digital currency.

19. (Currently Amended) The method of claim ~~1~~ 43 further comprising ~~the step of~~ verifying that the client has not exceeded a predetermined number of unsuccessful attempts to obtain the intermediate data.

20. (Currently Amended) The method of claim 19 wherein ~~the~~ verifying ~~step~~ further comprises:

transmitting a challenge code to the client; and

receiving the result of a cryptographic operation using the challenge code as an input and using a cryptographic key derived from the encrypted secret.

Claims 21-30. (Canceled).

31. (Currently Amended) ~~A~~ The method ~~for decrypting encrypted secrets associated with a client by a network server, the method~~ of claim 1, further comprising ~~the steps of~~:

~~receiving from a client a first secret;~~

~~transmitting client information to a first server, the client information derived from the first secret such that the first server can not feasibly determine the first secret;~~

~~receiving from the first server intermediate data, the intermediate data derived responsive to at least the client information and to a first server secret, wherein the intermediate data is derived by the second server such that the server secret cannot feasibly be determined;~~

deriving ~~a~~ the decryption key from the third secret ~~intermediate data~~; and

decrypting the encrypted secrets using the decryption key.

Claims 32-37 (Canceled)

38. (Currently Amended) A method for authenticating to a network server, the method comprising ~~the steps of~~:

~~transmitting to a first server client information derived from a first secret wherein the client information is derived such that the server can not feasibly determine the first secret;~~

~~receiving from the first server intermediate data, the intermediate data derived responsive to at least the received client information and to a server secret, wherein the intermediate data is derived such that the client can not feasibly determine the server secret;~~

implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the sever secret, wherein the protocol is implemented so that the client cannot feasibly determine the sever secret and the server cannot feasibly determine the client secret or the third secret;

at the client deriving a ~~server~~ password ~~by the client~~ from the ~~intermediate data~~ third secret and a server identifier;

authenticating to the network server using the ~~server~~ derived password, wherein the multi-party secure computation protocol implemented between the client and the server is the only multi-party computation protocol that is implemented in generating the third secret and the password derived from the third secret.

39. (Currently Amended) The method of claim 38 further comprising ~~the step of~~ transmitting to the first server by the network server verification that the user has authenticated successfully.

40. (Original) The method of claim 38 wherein the network server is a web server.

41. (Currently Amended) The method of claim 38 wherein ~~the~~ deriving ~~step~~ comprises deriving a server password using a key derivation function.

42. (Canceled)

43. (New) The method of claim 1, wherein implementing the multi-party secure computation protocol involves:

at the client, using the client secret to compute client information and then sending the client information to the server;

at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client; and

at the client, deriving the third secret from the intermediate data.

44. (New) The method of claim 1, wherein the multi-party secure computation protocol is a blind function evaluation protocol.

45. (New) The method of claim 44, wherein the blind function evaluation protocol is based on discrete-logarithm cryptography.

46. (New) The method of claim 45, wherein the blind function evaluation protocol is based on an RSA algorithm.

47. (New) A method for accessing encrypted data by a client, the method comprising:

implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the sever secret, wherein the protocol is implemented so that the client cannot feasibly determine the sever secret and the server cannot feasibly determine the client secret or the third secret;

authenticating the client by a device, the device storing encrypted secrets and configured not to provide the encrypted secrets without authentication; and

after authenticating, providing to the client by the device the encrypted secrets, wherein the encrypted secrets are capable of being decrypted using a decryption key derived from the third secret and wherein no additional multi-party secure computation protocol involving any entity other than the first server is required to enable the client to generate the third secret and the key derived from the third secret.